Abstract

Embodiments of the invention provide system and method of obfuscating data. According to one embodiment, a plurality of random numbers is generated by applying a one-way compression function to a plurality of auxiliary inputs which may at least include a secret key and a data partner identifier. Iteratively, for each row of data to be obfuscated, the following is performed: a plurality of data blocks is constructed from the each row of data to be obfuscated, wherein the number (n) of the data blocks is predetermined; a dot product is generated which is obtained by: generating a plurality of products by multiplying each of the plurality of data blocks with an exclusive one of the plurality of random numbers and summing the plurality of products; and an obfuscated form of the each row of data to be obfuscated is generated by determining a remainder of a modulo operation which is performed using the dot product as dividend and a predetermined integer value as divisor.

(Figure 2)